



State of California  
Office of the Attorney General

XAVIER BECERRA  
ATTORNEY GENERAL

August 20, 2020

*Via e-filing at [www.regulations.gov](http://www.regulations.gov)*

April J. Tabor, Acting Secretary of the Commission  
Federal Trade Commission  
Office of the Secretary  
600 Pennsylvania Avenue NW  
Suite CC-5610 (Annex B)  
Washington, DC 20580

RE: Comments on “FTC Health Breach Notification Rule, 16 CFR part 318, Project No. P20405,” 85 Fed. Reg. 31085 (May 22, 2020)

Dear Acting Secretary Tabor:

I write today in response to the Federal Trade Commission’s (“FTC”) request for public comment on its Health Breach Notification Rule (the “FTC Rule”), including whether the FTC Rule should be updated.<sup>15</sup> Recent technological and policy advances, including the increased use and development of telehealth apps and COVID-19 contact tracing apps, along with the passage of the Interoperability Rules, will put more consumer health data in the hands of non-Health Insurance Portability and Accountability Act (“HIPAA”) covered third parties. These parties are governed by the requirements of the FTC Rule. As such, I write to request that the FTC continue to align the requirements of the FTC Health Breach Notification Rule with those of the HIPAA Breach Notification Rule (the “HIPAA Rule”) and that the FTC broaden its definition of “breach” to mirror the HIPAA Rule, which is the baseline for health data privacy and security standards. Keeping the FTC Rule in line with the HIPAA Rule ensures the utmost protection for consumer health data and accomplishes Congress’s intent that that two rules remain complementary.

As California’s Attorney General, I have a duty to enforce consumer protection and health privacy laws to protect the public from losses that could result from the fraudulent use of

---

<sup>1</sup> FTC, 16 CFR Part 318 Health Breach Notification, 85 Fed. Reg. 31,085 (May 22, 2020) (explaining that the FTC reviews its guidance and regulations every 10 years to ensure that the Rule is keeping pace with technological and policy developments).

consumers' personal information obtained from a breach of health data. Protecting data privacy and security, especially of health data, is crucial to the financial health and well-being of consumers. Health data, in particular, is valuable and attractive to cybercriminals because medical records include Social Security information together with health information, opening up multiple avenues for criminal activity.<sup>2</sup> For example, cybercriminals have used information from stolen medical records, such as the individual's Social Security number and date of birth, to file fraudulent tax returns and to open credit cards, resulting in financial and reputational loss to affected consumers.<sup>3</sup> Victims of medical identity theft have also incurred out-of-pocket costs in order to restore their insurance coverage as well as increased insurance premiums after identity thieves incurred costly medical expenses using the stolen medical information.<sup>4</sup>

### **I. Alignment Between the Rules is critical to protecting consumer health data, especially in light of recent technological and policy developments**

When the FTC Health Breach Notification Rule was first enacted, entities that were not qualifying HIPAA covered entities or business associates had less opportunities to deal in health data because of then-current technological and policy landscapes. However, technology and

---

<sup>2</sup> Argaw, S.T., Bempong, N., Eshaya-Chauvin, B. *et al.*, *The State of Research on Cyberattacks Against Hospitals and Available Best Practice Recommendations: A Scoping Review*, BMC Medical Informatics and Decision Making (January 11, 2019), at 2, <https://doi.org/10.1186/s12911-018-0724-5>.

<sup>3</sup> Monica Beyer, *Hospital data breaches could lead to identity theft, financial fraud*, MedicalNewsToday.com (September 29, 2019), <https://www.medicalnewstoday.com/articles/326491> (Consumers whose medical records were compromised as a result of a hospital data breach reported experiencing financial and reputation loss.). In addition, health data could be held hostage for a hefty ransom by criminal enterprises. For example, on June 1, 2020, the University of California, San Francisco (“UCSF”), a leading medical research entity that is working on a cure for COVID-19, suffered a security attack against its medical school servers that was perpetrated by a criminal hacker group. UCSF reported the attack encrypted important public health-related academic work on the medical school servers. UCSF was forced to pay \$1.14 million in ransom to recover the data. Heather Landi, *UCSF pays hackers \$1.1M to regain access to medical school servers*, FierceHealthcare.com (July 1, 2020), <https://www.fiercehealthcare.com/tech/ucsf-pays-hackers-1-14m-to-regain-access-to-medical-school-servers>; Joe Tidy, *How hackers extorted \$1.14m from University of California, San Francisco*, BBCNews.com (June 29, 2020), <https://www.bbc.com/news/technology-53214783>.

<sup>4</sup> Experian, *The Potential Damages and Consequences of Medical Identity Theft and Healthcare Data Breaches*, Experian.com (April 2010), <https://www.experian.com/assets/data-breach/white-papers/consequences-medical-id-theft-healthcare.pdf>; Ponemon Institute, *2013 Survey on Medical Identity Theft*, Ponemon.org (September 2013), <https://www.ponemon.org/local/upload/file/2013%20Medical%20Identity%20Theft%20Report%20FINAL%2011.pdf>.

policy developments over the last decade mean that there are now more non-HIPAA covered entities and business associates dealing in health data, giving the FTC more opportunities to enforce the FTC Health Breach Notification Rule.<sup>5</sup>

The FTC anticipates that “as consumers turn toward direct-to-consumer technologies for health information and services (such as mobile health applications, virtual assistants, and platforms’ health tools), more companies may be covered by the FTC Health Breach Notification Rule.”<sup>6</sup> For example, technology-wise, an increasing number of contact tracing apps are entering the market due to the COVID-19 global pandemic, but it remains unclear whether these apps fall within HIPAA’s jurisdiction.<sup>7</sup> Policy trends suggest Congressmembers recognize this confusion and have proposed related legislation wherein the FTC, not HHS, has enforcement authority.<sup>8</sup> In addition, the enactment of the Final Interoperability Rules earlier this year opened the door for entities not covered by HIPAA to deal in health data.<sup>9</sup>

---

<sup>5</sup> Health apps have integrated into the daily life. Emily Vogels, *About one-in-five Americans use a smart watch or fitness tracker*, Pew Research Center (January 9, 2020), <https://www.pewresearch.org/fact-tank/2020/01/09/about-one-in-five-americans-use-a-smart-watch-or-fitness-tracker/>. See also e.g., Stephen Miller, *Apps Can Help Employees with Health Care*, Society for Human Resource Management | SHRM.com (March 2, 2020), <https://www.shrm.org/resourcesandtools/hr-topics/benefits/pages/apps-can-help-employees-with-health-care-.aspx> (Employees want employers to provide digital health apps that help employees maximize the value of their health and wellness benefits).

<sup>6</sup> 16 CFR Part 318 Health Breach Notification, 85 Fed. Reg. 31,085.

<sup>7</sup> Jane Anderson, *Report on Patient Privacy 20, no. 6, Experts warned that entities performing contact tracing for patients who have COVID-19 need to abide by HIPAA in some instances*, JDSupra, Healthcare Compliance Association (June 2020), <https://www.jdsupra.com/legalnews/report-on-patient-privacy-volume-20-39156/>.

<sup>8</sup> K. Smith, M. Stovsky, *Bipartisan Bill Seeks to Regulate COVID-19 Exposure Notifications*, JDSupra (July 14, 2020), <https://www.jdsupra.com/legalnews/bipartisan-bill-seeks-to-regulate-covid-85753/>.

<sup>9</sup> On March 9, 2020, the Centers for Medicare and Medicaid Services and the HHS Office of the National Coordinator for Health Information Technology (ONC) finalized the Interoperability Rules which are designed to make it easier for providers, insurers and patients to exchange electronic health data. See the CMS Interoperability and Patient Access Rule, <https://www.federalregister.gov/documents/2020/05/01/2020-05050/medicare-and-medicaid-programs-patient-protection-and-affordable-care-act-interoperability-and>; and ONC’s Cures Act Final Rule, <https://www.federalregister.gov/documents/2020/05/01/2020-07419/21st-century-cures-act-interoperability-information-blocking-and-the-onc-health-it-certification> (collectively, the “Interoperability Rules”). The Interoperability Rules require providers and insurers to adopt standardized application programming interfaces (“API”) – protocols that connect IT systems like electronic health records with third-party apps chosen by the patient whose records are being transferred. In turn, it becomes easier for providers, insurers, and patients to exchange health data across providers and across health systems and organizations. HHS clarified in sub-regulatory

Concerns about the privacy and security of health apps that collect and process consumers' health information are not hypothetical. Just recently, Walgreens reported that in January 2020, it discovered a software error in the Walgreens mobile app that allowed users to view the personal messages of other users stored within the Walgreens mobile app database.<sup>10</sup> As a result, health-related information was compromised, including customer names and prescription information. Walgreens did not report how many of its customers were impacted, but at the time the data breach was reported, the Walgreens app had over 10 million downloads on the Google Play Store. Another health app, the general practitioner telemedicine platform Babylon Health, suffered a data breach that enabled users to see other users' patient appointments and consultation information due to a software error.<sup>11</sup> While this breach only impacted a handful of app users, it raises concerns regarding the privacy and security of telehealth platforms, especially during this time of rapid expansion resulting from the COVID-19 global pandemic.

Thus, considering the current technological, policy, and business landscape, the FTC's role in health data privacy and security will be *more* prominent, and the protections of the FTC Health Breach Notification Rule for health data will be *more* important.

## **II. Congress intended for the FTC Rule to align with HIPAA requirements; the FTC should adopt the broader HIPAA definition for "breach"**

Congress intended for the HIPAA rule to be the baseline for health data privacy and security standards.<sup>12</sup> If the FTC Rule is updated in a manner that creates a misalignment with

---

guidance that once health information is received from a covered entity by an app chosen by the individual and the app was not provided by or on behalf of a covered entity, the transferred data is no longer protected by HIPAA. U.S. Department of Health and Human Services, Office for Civil Rights, *The access right health apps, & APIs*, HHS.gov, <https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/access-right-health-apps-apis/index.html> (last visited August 5, 2020). These third-party entities, however, continue to be subject to the FTC's authority. And so, in the event of a breach involving health data, these entities are required to conduct breach notification pursuant to the FTC Health Breach Notification Rule requirements, not the HIPAA Breach Notification Rule.

<sup>10</sup> Jessica Davis, *Walgreens Reports Data Breach from Personal Mobile Messaging App Error*, HealthITSecurity.com (March 02, 2020), <https://healthitsecurity.com/news/walgreens-reports-data-breach-from-personal-mobile-messaging-app-error>.

<sup>11</sup> Jessica Davis, *Breach of Telehealth App Babylon Health Raises Privacy Concerns*, HealthITSecurity.com (June 11, 2020), <https://healthitsecurity.com/news/breach-of-telehealth-app-babylon-health-raises-privacy-concerns>.

<sup>12</sup> The HITECH Act required the promulgation of two breach notification regulations—one from HHS for HIPAA covered entities and business associates, and another from the FTC for vendors of personal health records and non-HIPAA covered entities or business associates. American Recovery and Reinvestment Act of 2009, H.R. 1, 111th Cong. §§ 13402, 13407 (2009). Congress did so to "coordinate health information technology policy and programs of HHS with

HIPAA, entities dealing in health data could have different breach notification obligations for the same kind of data (health-related data). Consequently, consumers could no longer expect comparable health data breach notifications because the breach notification requirements could vary depending on who has custody of the health data.

The FTC Rule and the HIPAA Rule have intentionally similar requirements in order to maintain consistent compliance requirements for health data breach notification.<sup>13</sup> An entity would conduct breach notification pursuant to the requirements of either the FTC Health Breach Notification Rule or the HIPAA Breach Notification Rule, but rarely both.<sup>14</sup> 78 Fed. Reg. 5566, 5639. As a result, consumers now expect to receive breach notification for breaches involving their health data, informing them of the details of the breach, within a specific timeframe, regardless of whether the affected entity fell under the FTC or the HIPAA rule. Thus, continuing to align the two rules serves both consumer interests and Congressional intent for both rules to be complementary.

To sharpen the alignment of the two rules, the FTC should consider adopting the broader definition of breach under HIPAA so that entities' breach notification obligations are similar regardless of which rule is triggered. Under the HIPAA Rule, a breach occurs when data is acquired, access, used, or disclosed in a manner not permitted under HIPAA, unless the entity could demonstrate there was a low probability that the data was compromised, based on an assessment of 4 factors. 45 C.F.R. § 164.402. But under the FTC Rule, a breach occurs when data is acquired in an unauthorized manner, but presumes an accompanying unauthorized access unless the entity that suffered the breach can show otherwise. 16 C.F.R. § 318.2(a). The HIPAA Rule thus has a broader definition of what constitutes a breach because it treats any impermissible acquisition, access, use, or disclosure of health data as a breach, while the FTC Rule only treats an unauthorized acquisition as a breach. The FTC Health Breach Notification

---

other relevant executive branch agencies,” such as the FTC. H.R. 1 § 13101. Thus, continuing to align the FTC Health Breach Notification Rule and the HIPAA Breach Notification Rule would serve the purpose Congress intended for the rules to be complementary.

<sup>13</sup> See 16 C.F.R. § 318.2(a) (Breach Definition); 45 C.F.R. § 164.402 (Breach Definition); 16 C.F.R. § 318.4(a) (Timeliness of Breach Notification); 16 C.F.R. § 318.5(a) (Breach Notification to Individuals); 45 C.F.R. § 164.404(d)(2) (Breach Notification to Individuals); 16 C.F.R. § 318.5(b) (Breach Notification to the Media); 45 C.F.R. § 164.406 (Breach Notification to the Media); 16 C.F.R. § 318.5(c) (Breach Notification to the Enforcing Agency); 45 C.F.R. § 164.408 (Breach Notification to the Enforcing Agency).

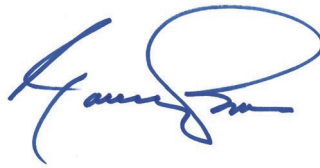
<sup>14</sup> See Federal Trade Commission, *Complying with the FTC's Health Breach Notification Rule*, <https://www.ftc.gov/tips-advice/business-center/guidance/complying-ftcs-health-breach-notification-rule> (Many web-based businesses that collect consumer health information are not covered by HIPAA. The FTC issued the FTC Health Breach Notification Rule to require certain businesses not covered by HIPAA to notify their customers and others if there is a breach of unsecured, individually identifiable electronic health information.).

Rule would benefit from a broader definition of breach to ensure that the breach notification obligations of entities are similarly triggered under comparable fact patterns.

### **III. Conclusion**

Continuing to align the requirements of the FTC Health Breach Notification Rule with the requirements of the HIPAA Breach Notification Rule ensures that consumer health data is subject to comparable breach notification requirements and protocols regardless of the type of entity that has custody of the data. This benefits consumers and serves Congress's intent.

Sincerely,

A handwritten signature in blue ink, appearing to read "Xavier Becerra", with a large, stylized loop at the end.

XAVIER BECERRA  
California Attorney General